UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/800,983	03/15/2004	G. Glenn Henry	CNTR.2073	1410

23669 7590 03/21/2007
HUFFMAN LAW GROUP, P.C.
1900 MESA AVE.
COLORADO SPRINGS, CO 80906

EXAMINER	
TRAORE, FATOUMATA	
ART UNIT	PAPER NUMBER
2109	

SHORTENED STATUTORY PERIOD OF RESPONSE	NOTIFICATION DATE	DELIVERY MODE
3 MONTHS	03/21/2007	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Notice of this Office communication was sent electronically on the above-indicated "Notification Date" and has a shortened statutory period for reply of 3 MONTHS from 03/21/2007.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

PTO@HUFFMANLAW.NET

Office Action Summary	Application No.	Applicant(s)	
	10/800,983	HENRY ET AL.	
	Examiner	Art Unit	
	Fatoumata Traore	2109	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *15 March 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-26* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-26* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *15 March 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *See Continuation Sheet*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

Continuation of Attachment(s) 3). Information Disclosure Statement(s) (PTO/SB/08), Paper No(s)/Mail Date :, 2007-01-25, 2006-11-03, 2006-09-30, 2006-07-25, 2006-06-05, 2006-06-04, 2006-03-18 , 2006-03-11, 2005-09-25, 2005-04-16, 2004-03-15.

DETAILED ACTION

This action is in response of the original filing of March 15, 2004. Claims 1-26 are pending and have been considered below.

Claim Rejections - 35 USC § 101

1. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 1-26 are rejected under 35 U.S.C. 101 because the claim are directed to non-statutory subject matter.

Regarding claims 1-21, although the preamble of the claims recite "apparatus" the body of the claims include only software components such as "a cryptographic instruction", "keygen logic", and "execution logic". Claims 1-21 neither includes any computer hardware component(s) nor positively recites that the cited software components are stored on a computer medium that can be read by a machine. As such, claims 1-21 are directed to software per se which is non-functional descriptive material and non-statutory since the claims do not require any physical transformation and the invention as claimed does not produce a useful, concrete, and tangible result to form the basis of statutory subject matter under 35 U.S.C 101.

Regarding claims 22-26, the method as claimed does not provide a tangible result to form the basis of statutory subject matter under 35 U.S.C. 101.

Claim Rejections - 35 USC § 112

2. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

3. Claims 9, 10, 12, 14, 15 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter, which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. Specifically,

"Regarding claim 9, "a first register, wherein contents of said first register comprise a first pointer to a first memory address, said first memory address specifying a first location in memory for access of said plurality of input text blocks" was not described in the specification.

Regarding claim 10, "the plurality of registers comprises: a second register, wherein contents of said second register comprise a second pointer to a second memory address, said second memory address specifying a second location in said memory" was not described in the specification.

Regarding claim 12, "a fourth register, wherein contents of said fourth register comprise a third pointer to a third memory address, said third memory address specifying a third location in memory for access of cryptographic key data" was not described in the specification.

Regarding claim 14, "the plurality of registers comprises: a fifth register, wherein contents of said fifth register comprise a fourth pointer to a fourth memory address, said fourth memory address specifying a fourth location in memory, said fourth location comprising said initialization vector location" was not described in the specification.

Regarding claim 15, "the plurality of registers comprises: a sixth register, wherein contents of said sixth register comprise a fifth pointer to a fifth memory address, said fifth memory address specifying a fifth location in memory " was not described in the specification.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

5. Claims 1-4, 6, 8, 16-18, 20, 22-24 are rejected under 35 U.S.C. 102(b) as being anticipated by **Ehrsam et al** (US 4386234).

Claim 1: **Ehrsam et al** discloses a cryptographic apparatus for performing cryptographic operation comprising:

i. A cryptographic instruction, received by a computing device as part of an instruction flow executing on said computing device, wherein said cryptographic instruction prescribes one of the cryptographic operations, and wherein said cryptographic instruction prescribes that a user-

generated key schedule be employed for execution of said one of the cryptographic operations (the terminal data security device also provides an arrangement which permits a variety of applications using a pre-defined private data encryption key) (column 5, lines 63-65);

ii. Keygen logic, operatively coupled to said cryptographic instruction, configured to direct said computing device to load said user-generated key schedule (with a load key direct operation request to the interface adapter the private data encryption key is loaded directly into the working register) (column 5, lines 65-68);

iii. And execution logic, operatively coupled to said keygen logic, configured to employ said user-generated key schedule to execute said one of the cryptographic operations (this allows subsequent encipher/decipher operations to proceed under control of the private data encrypting key) (column 6, lines 1-5).

Claims 17, 22: **Ehrsam et al** discloses a cryptographic apparatus and method for performing cryptographic operation comprising:

i. A cryptography unit within a device, configured to execute one of the cryptographic operations responsive to receipt of a cryptographic instruction within an instruction flow that prescribes said one of the cryptographic operations, wherein said cryptographic instruction also prescribes that a user-generated key schedule be employed when

executing said one of the cryptographic operations (the terminal data security device also provides an arrangement which permits a variety of applications using a pre-defined private data encryption key) (column 5, lines 63-65);

ii. And keygen logic, operatively coupled to said cryptography unit, configured to direct said device to perform said one of the cryptographic operations and to employ said user-generated key schedule when performing said one of the cryptographic operations (This allows subsequent encipher/decipher operations to proceed under control of the private data encrypting key) (column 6, lines 1-5).

Claim 2: **Ehrsam et al** discloses a cryptographic apparatus for performing cryptographic operation as in claim 1 above, and further discloses that the one of the cryptographic operations further comprises: an encryption operation, said encryption operation comprising encryption of a plurality of plaintext blocks to generate a corresponding plurality of ciphertext blocks (still another object of the invention is to provide a terminal cryptographic facility for performing an encipher function for enciphering input plaintext under control of data encrypting key stored in the working key register to produce output cipher text) (column 4, lines 21-26).

Claim 3: **Ehrsam et al** discloses a cryptographic apparatus for performing cryptographic operation as in claim 1 above, and further discloses that the one of the cryptographic operations further comprises: a decryption operation, said decryption operation comprising decryption of a plurality of ciphertext blocks to generate a corresponding plurality of plaintext blocks (still a further object of the invention is to provide a terminal cryptographic facility for performing a decipher function for deciphering input ciphertext under control of data encrypting key stored in a working key register to produce output plaintext) (column 4, lines 26-32).

Claims 4, 18, 24: **Ehrsam et al** discloses a cryptographic apparatus and method for performing cryptographic operation as in claims 1, 17, and 22 above, and further discloses that the said user-generated key schedule is stored in memory (the terminal has an integrated data security device which includes a memory for storing a terminal master key) (column 5, lines 25-30).

Claims 6, 20, 23: **Ehrsam et al** discloses a cryptographic apparatus and method for performing cryptographic operation as in claims 1, 17, and 22 above, and further discloses that the keygen logic is configured to interpret a key generation field within a control word which is referenced by said cryptographic instruction (key generation includes the specification of a system master key, primary and secondary communication keys and the primary file key. The master key is used

by the cryptographic apparatus for internal deciphering enciphering keys which can be used as the working key in subsequent encipher/decipher operation) (column 9, lines 33-60).

Claim 8: **Ehrsam et al** discloses a cryptographic apparatus for performing cryptographic operation as in claim 1 above, and further discloses that the cryptographic instruction implicitly references a plurality of registers within said computing device (the buffer register is provided with parallel input and output paths from and to a 64 bit data register also divided into upper and lower data registers) (column 14, lines 40-45).

Claim 16: **Ehrsam et al** discloses a cryptographic apparatus for performing cryptographic operation as in claim 1 above, and further discloses that the execution logic comprises: a cryptography unit, configured execute a plurality of cryptographic rounds on each of said plurality of input text blocks to generate a corresponding each of a plurality of output text blocks, wherein said plurality of cryptographic rounds are prescribed by a control word that is provided to said cryptography unit During each round of the cipher function, the data contents of the upper data register is enciphered under control of the working key register, with the result being added modulo 2 to the contents of the lower data register) (column 15, lines 42-46).

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 5, 19, 25 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Ehrsam et al** (US 4386234) in view of **Fischer et al** (CHES 2001, LNCS 2162, pp 77-92, 2001).

Claims 5, 19, and 25: **Ehrsam et al** discloses a cryptographic apparatus and method for performing cryptographic operation as in claims 1, 17, and 22 above, but does not explicitly disclose that the user-generated key schedule comprises an expanded key schedule according to the Advanced Encryption Standard (AES) algorithm. However, **Fischer et al** discloses a key schedule using the advanced encryption standard (in October 2000, NIST has decided to propose Rijndael cipher as the advanced encryption standard) (page 78 paragraph 1, and figure 2). Therefore, it would have been obvious to one having ordinary skill in the art at the time of the invention for **Ehrsam et al** to use the advance encryption standard. One would have been motivated to do so in order to secure their data from internal and external threats.

8. Claims 7, 21, 26 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Ehrsam et al** (US 4386234) in view of **Neuman et al** (US 2002/0162026).

Claims 7, 21, and 26: **Ehrsam et al** discloses a cryptographic apparatus and method for performing cryptographic operation as in claims 1, 17, and 22 above, but does not explicitly disclose that the cryptographic instruction is prescribed according to the x86 instruction format. However, **Neuman et al** discloses an apparatus and method for providing secure network communication which further discloses that the cryptographic instruction is prescribed according to the x86 instruction format (a processor other than the AU1000 can be used, such as a StrongARM, SH-4, x86, etc) (page 7, paragraph [102}). Therefore, it would have been obvious to one having ordinary skill in the art at the time of the invention for **Ehrsam et al** to use an x86 processor. One would have been motivated to do so in order to have more memory space.

9. Claims 9-15 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Ehrsam et al** (US 4386234) in view of **Cooney** (US 488802).

Claim 9: **Ehrsam et al** discloses a cryptographic apparatus and method for performing cryptographic operation as in claim 8 above, but does not explicitly disclose that the plurality of registers comprises: a first register, wherein contents of said first register comprise a first pointer to a first memory address, said first memory address specifying a first location in memory for access of said plurality of input text blocks upon which said one of the cryptographic operations is to be

accomplished. However, **Cooney** discloses a system for storing encrypter keys in a secure manner further discloses an input register (the terminal through its application program will load the clear text key in the encrypt register via the auxiliary and thereafter, the data to be encrypted is loaded into the input register via the master port) (column 4, lines 60-65). Therefore, it would have been obvious to one having ordinary skill in the art at the time of the invention for **Ehrsam et al** to have an input register. One would have been motivated to do so in order to preserve the input information for retrieval.

Claim 10: **Ehrsam et al** discloses a cryptographic apparatus and method for performing cryptographic operation as in claim 8 above, but does not explicitly disclose that the plurality of registers comprises: a second register, wherein contents of said second register comprise a second pointer to a second memory address, said second memory address specifying a second location in said memory for storage of a corresponding plurality of output text blocks, said corresponding plurality of output text blocks being generated as a result of accomplishing said one of the cryptographic operations upon a plurality of input text blocks. However, **Cooney** discloses a system for storing encrypter keys in a secure manner further discloses an output register (the encrypted data is then transferred to the output register) (column 5, lines 1-5). Therefore, it would have been obvious to one having ordinary skill in the art at the time of the invention for

Ehrsam et al to have an output register. One would have been motivated to do so in order to preserve the output information for retrieval.

Claim 11: **Ehrsam et al** discloses a cryptographic apparatus and method for performing cryptographic operation as in claim 8 above, but does not explicitly disclose that the plurality of registers comprises: a third register, wherein contents of said third register indicate a number of text blocks within a plurality of input text blocks. However, **Cooney** discloses a system for storing encrypter keys in a secure manner further discloses a mode status register (the mode status register is used to inform host CPU as to the status of the enciphering chip (number of input lock)) (column 7, lines 28-29). Therefore, it would have been obvious to one having ordinary skill in the art at the time of the invention for **Ehrsam et al** to have a status register. One would have been motivated to do so in order to preserve the status information for retrieval.

Claim 12: **Ehrsam et al** discloses a cryptographic apparatus and method for performing cryptographic operation as in claim 8 above, but does not explicitly disclose that the plurality of registers comprises: a fourth register, wherein contents of said fourth register comprise a third pointer to a third memory address, said third memory address specifying a third location in memory for access of cryptographic key data for use in accomplishing said one of the cryptographic operations. However, **Cooney** discloses a system for storing

encrypter keys in a secure manner further discloses cryptographic key (the command register tells the enciphering chip what function it is to perform) (column 7, lines 30-31). Therefore, it would have been obvious to one having ordinary skill in the art at the time of the invention for **Ehrsam et al** to have a key register. One would have been motivated to do so in order to preserve the cryptographic keys information for retrieval.

Claim 13: **Ehrsam et al** and Cooney disclose a cryptographic apparatus and method for performing cryptographic operation as in claim 12 above, and **Cooney** further discloses that the user-generated key schedule comprises said cryptographic key data (with a load key direct operation request to the interface adapter the private data encryption key is loaded directly into the working register) (column 5, lines 65-70).

Claim 14: **Ehrsam et al** discloses a cryptographic apparatus and method for performing cryptographic operation as in claim 8 above, but does not explicitly disclose that the plurality of registers comprises: a fifth register, wherein contents of said fifth register comprise a fourth pointer to a fourth memory address, said fourth memory address specifying a fourth location in memory, said fourth location comprising said initialization vector location, contents of said initialization vector location comprising an initialization vector or initialization vector equivalent for use in accomplishing said one of the cryptographic operations. However,

Cooney discloses a system for storing encrypter keys in a secure manner further discloses an initialization vector register (another characteristic of the chip is that it permits the initialization vector encrypt and decrypt registers to be read by the host CPU) (column 7, lines 65-68). Therefore, it would have been obvious to one having ordinary skill in the art at the time of the invention for **Ehrsam et al** to have initialization vector register. One would have been motivated to do so in order to preserve the initialization vector information for retrieval.

Claim 15: **Ehrsam et al** discloses a cryptographic apparatus and method for performing cryptographic operation as in claim 8 above, but does not explicitly disclose that the plurality of registers comprises: a sixth register, wherein contents of said sixth register comprise a fifth pointer to a fifth memory address, said fifth memory address specifying a fifth location in memory for access of a control word for use in accomplishing said one of the cryptographic operations, wherein said control word prescribes cryptographic parameters for said one of the cryptographic operations, and wherein said control word comprises: a keygen field, configured to specify that said user-generated key schedule be employed during execution of said one of the cryptographic operations. However, **Cooney** discloses a system for storing encrypter keys in a secure manner further discloses control register (a working key is defined as a key to encrypt or decrypt data) (column 10, lines 1-20). Therefore, it would have been obvious to one having ordinary skill in the art at the time of the invention for **Ehrsam et al** to

have control key register. One would have been motivated to do so in order to preserve the control key information for retrieval.

Conclusion

10. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Best (US 4319079) Crypto microprocessor using cipher.

b. Hember (US 5633934) Local area network encryption decryption system.

c. McCarty (US 5666411) System for computer software protection.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Fatoumata Traore whose telephone number is (571) 270-1685. The examiner can normally be reached Monday through Thursday from 7:30 a.m. to 4:30 p.m. and every other Friday from 7:30 a.m. to 3:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jim W. Myhre, can be reached on (571) 272 6722. The fax phone number for Formal or Official faxes to Technology Center 2100 is (571) 273-3800. Draft or Informal faxes, which will not be entered in the application, may be submitted directly to the examiner at (571) 274-1685.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the Group Receptionist whose telephone number is (571) 272-2100.

FT
March 12, 2007

James W. Myhre
Supervisory Patent Examiner